Over the last several years, the Office of the Program Manager for the Information Sharing Environment (PM-ISE) has worked with Critical Infrastructure and Key Resources (CIKR) community partners in support of national security, public safety, and economic resilience. PM-ISE's stewardship, information sharing technical expertise, advocacy efforts, and policy and governance tools in support of partners' information sharing needs have contributed to the improvement of information sharing within the public domain. Recent project work includes Project Interoperability in Puget Sound; a Maritime Data Challenge to combat illegal, unreported, and unregulated fishing; the development of a Maritime Domain Awareness Architecture Plan; a pilot study to look at the impacts of international mass migration on the maritime domain; an insider threat and risk analysis pilot; and an effort to team fusion center resources with the energy sector.

**Project Interoperability in Puget Sound**

PM-ISE is teaming with the National Maritime Intelligence-Integration Office (NMIO) and The University of Washington's Center for Collaborative Systems for Security, Safety and Regional Resilience (CoSSaR) to work with port partners to develop technology to permit the real-time situational awareness and information sharing of relevant data, such as vessel arrival, emergency response, and notification data. The Puget Sound community was selected for the project because it is a model of regional complexity. A connected system of waterways and communities in Northwest Washington, any disruption to the security of Puget Sound's maritime industry could impact its $30 billion contribution to Washington State's economy and the 148,000 jobs it provides directly and indirectly to the region. With seven ports and an international border, Puget Sound offers opportunities to observe and research the alignment of information flows, information technology, and communication systems employed in support of daily operations across numerous federal, state, local, tribal, international, public, and private

entities—all of whom are key stakeholders.

CoSSaR is leading the effort to move forward Project Interoperability (PI), a suite of technological tools and resources for improving information interoperability across multiple organizations and IT systems. Federated Identity, Credential, and Access Management (ICAM), a PI tool, is the set of technological security disciplines, policies, and processes that establish trust and interoperability among organizations that want to share information such as incident management, homeland security, and law enforcement. These organizations look for assurances that partners with whom they wish to share information are implementing policies and standards in a manner worthy of trust and that support interoperability before information sharing can occur. The Federated ICAM landscape includes information sharing at the Sensitive But Unclassified (SBU) level of information access, allowing mission partners at the federal, state, and local levels as well as private sector participants to share information. This concept will allow Puget Sound partners to better achieve the situational awareness and the information sharing requirements necessary to support the physical and economic security of the maritime community. To learn more about CoSSaR's work, refer to this ISE blog post. Project Interoperability in Puget Sound will conclude at the end of FY16.

**Maritime Data Challenge**

PM-ISE is also teaming with NMIO as a co-sponsor of a global data challenge designed to combat illegal, unreported, and unregulated (IUU) fishing. This effort is conducted under the White House's Challenge.gov crowd-sourcing problem-solving initiative. By applying innovative analytic techniques to existing data sets, this data challenge seeks to develop a process, available to all, to more effectively identify and react to the global IUU fishing threat. The objective of this effort is to develop an unclassified algorithm identifying behavior(s) of vessels engaged in fishing, and enable decision makers to identify those vessels engaged in IUU fishing activity in order to best deploy limited enforcement resources. The U.S. Government intends to make this algorithm freely available to all legitimate maritime stakeholders to include foreign governments, non-governmental organizations, etc.

**Maritime Domain Awareness Mass Population Pilot**

PM-ISE is teaming with the Open Geospatial Consortium (OGC) to conduct a Maritime Mass Migration Information Sharing Pilot. The pilot will focus on the coordination challenges of multi-regional and multi-national operations and will work to understand cross-domain interoperability on an international level in a maritime context. The scenario will include a range of information

sources and technologies relevant to the movement of people from the Middle East to Europe. The pilot will include the exchange of information relevant to maritime domain awareness.

**National Maritime Domain Awareness Architecture Plan**

PM-ISE collaborated with the mission partners of the Maritime Domain Awareness Executive Steering Committee (MDA ESC), including the Department of Defense (DoD), Department of Homeland Security (DHS), Department of Transportation, and NMIO to draft, secure the endorsement of, and issue the National Maritime Domain Awareness (MDA) Architecture Plan. The MDA Architecture Plan culminates a four-year effort to improve data exchange efforts among U.S. Government agencies. Additionally, the plan aligns with the Information Interoperability Framework (I2F) to implement the National Information Exchange Model (NIEM) as the maritime data standard, and outlines a maritime information sharing environment enterprise concept to enable web and cloud-based information sharing among maritime vessels, cargo, people, and infrastructure within the Global Maritime Community of Interest.

**DSS Threat and Risk Analysis Project**

PM-ISE is partnering with the Defense Security Service (DSS) to apply existing information sharing frameworks and standards to develop a data dictionary and standardized architecture for DSS's information technology (IT) systems. Currently, there is not a common business model to allow the automatic sharing of information between DSS disparate IT networks and data layers that support its various stakeholders including the National Industrial Security System (NISS), Office of Designated Approving Authority (ODAA) Business Management System (OBMS), Analysis, Research, Case Tracking, and Collaboration (ARCTC), and Defense Insider Threat Management and Analysis Center (DITMAC).

The joint threat and risk initiative seeks to use NIEM and Object Management Group (OMG) threat and risk modeling to create a data dictionary of standard vocabulary for DSS' IT systems. NIEM assists users in adopting a standards-based approach to exchanging data by creating a data dictionary of agreed-upon terms, definitions, relationships, and formats as well as a project management framework to implement a standardized data model approach[1]. OMG threat and risk modeling builds upon NIEM's approach by taking the standardized data and mapping it to multiple exchange schema so that analytics can be applied using multiple data sources[2]. This approach to standardized data architecture will be used to support insider threat investigations within DSS and its oversight of cleared government contractors and companies.

**NFCA/E-ISAC Rapid Deployment Project**

PM-ISE is working with the National Fusion Center Association (NFCA) and the Electricity Information Sharing and Analysis Center (E-ISAC) to consider utilizing the national fusion center network to rapidly convene electrical infrastructure subject matter experts (SMEs) in the event of an emergency power grid failure. Fusion centers are localized information sharing hubs that bring together federal, state, local, tribal, and territorial (FSLTT) partners. They collaborate with the Department of Homeland Security (DHS) to coordinate the homeland security and intelligence efforts of the FSLTT partners. This structure is ideal to hosting SMEs who, depending on the scale and complexity of an incident, need access to classified data in order to inform their recommendations. This effort also has the potential to develop into a long-term information exchange relationship between the energy sector and fusion centers to provide situational awareness of threats and vulnerabilities in their areas of responsibility. It represents an incremental, collaborative approach to facilitating a lasting relationship between these communities of interest that currently do not have frequent interaction.

In order to support maritime and critical infrastructure information sharing of FSLTT partners, an emphasis has been made on supporting the development of an enterprise architecture approach. This approach supports interoperability among partners' data systems through data architecture and the federation of user identities to facilitate information sharing and interagency coordination. The mission partners of the CIKR community will continue to work together to leverage PI, Federated ICAM, and other technological capabilities to improve the efficiency and resiliency of the ISE.

[1] https://www.niem.gov/aboutniem/Pages/niem.aspx

[2] http://www.omg.org/hot-topics/threat-modeling.htm